IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Raikar	Patent Application	
Serial No.:	10/722,822	Group Art Unit:	2136
Filed:	11/25/2003	Examiner: Hoffman, Brandon S.	

For: DYNAMIC SOURCE AUTHENTICATION AND ENCRYPTION CRYPTOGRAPHIC SCHEME FOR A GROUP BASED COMMUNICATION ENVIRONMENT

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-26 stand rejected. Rejections of claims 1-26 are herein appealed.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a method (method 500 of Figure 5 and page 16, lines 6-9) for establishing secure group-based communication. The method (method 500 of Figure 5) includes distributing (502 of Figure 5 and page 16, lines 9-13) a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts. The method 500 further includes distributing (504 of Figure 5 and page 16, lines 15-21) a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

Independent Claim 10 recites a method (500 of Figure 5 and page 16, lines 6-9) for establishing a secure group-based communication environment between a plurality of hosts. The method (500 of Figure 5 and page 16, lines 6-9) includes distributing (502 of Figure 5 and page 16, lines 9-13) a first set of keys to each of said plurality of hosts for encrypting communication between said hosts and for authenticating a source of communication between said plurality of hosts. The method 500 also includes distributing (506 of Figure 5 and page 16 line 22 through page 17, line 6) a subset of said first set of keys to each of said plurality of hosts for validating said source of communication between said plurality of hosts. The method further includes distributing (504 of Figure 5 and page 16, lines 15-21) a second set of keys to each of said plurality of hosts for dynamically modifying said first set of keys and said subset of said first set of keys.

Independent Claim 18 provides a computer readable medium comprising executable instructions which, when executed in a processing system (12 of Figure 6 and page 19, line 4 through page 20, line 13), causes the system to perform the steps for a method (method 500 of Figure 5 and page 16, lines 6-9) of establishing secure group-based communication. The method 500 includes distributing (502 of Figure 5 and page 16, lines 9-13) a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts. The method 500 also includes distributing (504 of Figure 5 and page 16, lines 15-21) a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-26 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent pub. No. 2002/0154776 by Sowa et al. (referred to hereinafter as "Sowa").

Arguments

1. Whether Claims 1-26 are anticipated by U.S. Patent Pub. No. 2002/0154776 by Sowa et al. (referred to hereinafter as "Sowa").

Appellants respectfully submit that embodiments of the present invention are not anticipated by Sowa and respectfully appeal the rejection.

Independent Claim 1 recites an embodiment of the present invention directed to (emphasis added):

A method for establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

Independent Claims 10 and 18 recites similar features. Claims 2-9 that depend from independent Claim 1, Claims 11-17 that depend from Claim 10 and Claims 19-26 that depend from Claim 18 also include these features.

MPEP §2131 provides (emphasis added):

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). … "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor*

Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Appellants respectfully submit that Sowa fails to teach or suggest "distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts," as claimed. The Examiner has cited paragraph [0044] as teaching this feature. However, in contrast to the Examiner's interpretation of this passage, Appellants submit that Sowa teaches "the CCK has no relation to a particular talk group (TG)."

Appellants submit that the CCK of Sowa is not intended to be used to "authenticate group-based communication," as claimed, since the CCK of Sowa "has no relation to a particular talk group (TG)." As such, Appellants do not understand Sowa as teaching this claimed feature of the present invention.

In the "response to arguments" portion of the current Office Action, the Examiner has suggested that a geographic location defines a group. Appellants respectfully submit that Sowa directly teaches away from the Examiner's interpretation and that by characterizing a geographic location as a group communication makes an anticipation rejection improper. Sowa specifically states the CCK has no relation to a talk group and any interpretation of this teaching should be made as an obviousness rejection, not an anticipation rejection.

Additionally, Sowa in paragraph 101 states "it is possible for more than one location area to have the same CCK." Appellants do not understand how a geographic location can be considered a communication group when a different location can have the same CCK.

Furthermore, Appellants submit that Sowa fails to teach or suggest the feature of "distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys," as claimed. With the claimed invention, the second set of keys is distributed to the hosts for dynamically modifying the first set of keys that are used for authentication of group-based communication. With the present invention, the group that receives the first set of keys also receives the second set of keys to dynamically modify the first set of keys. This is not true of Sowa.

The Examiner has relied on paragraph [0045] as teaching this feature and the Appellants respectfully disagrees that Sowa teaches or suggests this feature. In paragraph [0045], Sowa teaches "a GCK is defined for each talk group in the system." Appellants submits that the GCK of Sowa does not dynamically modify the CCK (e.g., first set of keys) because the CCK has "no relation to a particular talk group" while the GCK is "defined for a particular talk group."

Furthermore, in paragraph [0045] Sowa states "the GCK is only indirectly used for the encryption of traffic information." Sowa fails to teach or suggest "dynamically modifying said first set of keys" with the second set of keys, as claimed.

Appellants submit that Sowa fails to teach each element of Independent Claim 1. Independent Claim 10 and 18 recites similar features. As such, Appellants respectfully assert that Claims 1-26 are not anticipated by Sowa and respectfully request the rejection to Claims 1-26 is improper and should be removed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 4/18/2008

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNER BLECHER LLP
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0500

Claims Appendix

1. A method for establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

2. The method as recited in Claim 1 further comprising:

distributing said second set of keys wherein a unique set of keys are distributed to each of said plurality of hosts.

3. The method as recited in Claim 2 further comprising:

distributing said second set of keys wherein each of said plurality of hosts receives a unique key for each of said plurality of hosts except for itself.

4. The method as recited in Claim 1 further comprising:

communicating between said hosts in a utility data center communications environment.

5. The method as recited in Claim 1 further comprising:

authenticating a communication source from a host level.

6. The method as recited in Claim 1 further comprising:

authenticating a communication source from an application level.

7. The method as recited in Claim 1 further comprising:

adding a new host to said plurality of hosts and dynamically modifying said first set of keys in response to adding said new host.

8. The method as recited in Claim 1 further comprising:

in response to removing one of said plurality of hosts, dynamically modifying said first set of keys.

9. The method as recited in Claim 1 further comprising:

dynamically modifying said first set of keys at regular intervals with said second set of keys.

10. A method for establishing a secure group-based communication environment between a plurality of hosts comprising:

distributing a first set of keys to each of said plurality of hosts for encrypting communication between said hosts and for authenticating a source of communication between said plurality of hosts;

distributing a subset of said first set of keys to each of said plurality of hosts for validating said source of communication between said plurality of hosts; and

distributing a second set of keys to each of said plurality of hosts for dynamically modifying said first set of keys and said subset of said first set of keys.

11. The method as recited in Claim 10 further comprising:

adding a new host to said plurality of hosts; and

dynamically modifying said first set of keys and said subset of said first set of keys.

12. The method as recited in Claim 11 further comprising:

dynamically modifying said first set of keys and said subset of said first set of keys with a third set of keys generated in response to adding said new host.

13. The method as recited in Claim 10 further comprising:

removing a host from said plurality of hosts;

dynamically modifying said first set of keys and said subset of said first set of keys.

14. The method as recited in Claim 13 further comprising:

dynamically modifying said first set of keys and said subset of said first set of keys with a third set of keys generated in response to removing said host from said plurality of hosts.

15. The method as recited in Claim 10 further comprising:

communicating between said plurality of hosts in a utility data center communications environment.

16. The method as recited in Claim 10 further comprising:

validating said source of communication between said plurality of hosts at a host level.

17. The method as recited in Claim 10 further comprising:

validating said source of communication between said plurality of hosts at an application level.

18. A computer readable medium comprising executable instructions which, when executed in a processing system, causes the system to perform the steps for a method of establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

19. The computer readable medium as recited in Claim 18 wherein said method further comprises:

distributing said second set of keys wherein a unique set of keys are distributed to each of said plurality of hosts.

20. The computer readable medium as recited in Claim 19 wherein said method further comprises:

distributing said second set of keys wherein each of said plurality of hosts receives a unique key for each of said plurality of hosts except for itself.

21. The computer readable medium as recited in Claim 18 wherein said method further comprises:

communicating between said hosts in a utility data center communications environment.

22. The computer readable medium as recited in Claim 18 wherein said method further comprises:

authenticating a communication source from a host level.

23. The computer readable medium as recited in Claim 18 wherein said method further comprises:

authenticating a communication source from an application level.

24. The computer readable medium as recited in Claim 18 wherein said method further comprises:

adding a new host to said plurality of hosts and dynamically modifying said first set of keys in response to adding said new host.

25. The computer readable medium as recited in Claim 18 wherein said method further comprises:

in response to removing one of said plurality of hosts, dynamically modifying said first set of keys.

26. The computer readable medium as recited in Claim 18 wherein said method further comprises:

dynamically modifying said first set of keys at regular intervals with said second set of keys.

Evidence Appendix

None

Related Proceedings Appendix

None